CLAIMS

1. Authentication method of at least one application working in a equipment connected by a network to a control server, said equipment being locally connected to a security module, said application is loaded and/or executed by means of an application execution environment of the equipment and uses resources stored in the security module, comprising the following preliminary steps:

- reception by the control server, via the network, of data comprising at least the identifier of the equipment and the identifier of the security module,

- analysis and verification by the control server of said data,

- generation of a cryptogram comprising a digest of the application, data identifying the equipment and the security module and instructions intended for said module,

- transmission of said cryptogram, via the network and the equipment, to the security module,

- verification of the application by comparing the digest extracted from the cryptogram received with a digest determined by the security module,

said method further comprising steps wherein, during the initialization and/or the activation of the application, the security module executes the instructions extracted from the cryptogram and releases, respectively blocks the access to certain resources of said security module according to the result of the verification suited to this application carried out previously.

2. Method according to claim 1 wherein the equipment is a mobile equipment of mobile telephony.

3. Method according to claim 1 wherein the network is a mobile network of the type GSM or GPRS or UMTS.

4. Method according to claim 1 or 2, wherein the security module is a subscriber module inserted into the mobile equipment of mobile telephony of the SIM card type.

5. Method according to claim 4 wherein the identification of the set mobile equipment / subscriber module is carried out from the identifier of the mobile equipment and from the identifier of the subscriber module suited to a subscriber to the network.

6. Method according to claim 1 wherein the instructions included in the cryptogram received by the security module condition the use of the applications according to criteria established previously by the operator an/or the application supplier and/or the user of the equipment.

7. Method according to claim 6 wherein the criteria defining the limits of use of an application according to the risks associated with the software of said application or with the hardware of the equipment that the operator desires to take into account.

8. Method according to claim 1 wherein the verification of the application with the cryptogram is carried out at the time of the first initialization or at the time of the first use of said application.

9. Method according to claim 1 wherein the verification of the application with the cryptogram is periodically carried out at a given rate according to instructions originating from the control server.

10. Method according to claim 1 wherein the verification of the application with the cryptogram is carried out at the time of each initialization of said application on the equipment.

11. Method according to claim 1 wherein the cryptogram is generated with the aid of an asymmetrical or symmetrical encryption key from a data set containing, among other data, the identifier of the equipment, the identifier of the security module, an identifier of the application, the digest of the application calculated with an unidirectional hash function and identifiers of the resources of the security module and instructions for locking/releasing of resources of the security module.

12. Method according to claim 11 wherein the cryptogram includes a variable that is predictable by the security module avoiding the double use of a same cryptogram, the value of said variable being controlled by the security module by making a

comparison with that of a reference value stored in said module and regularly updated.

13. Method according to claim 1 wherein the security module transmits to the control server, via the equipment and the network, a confirmation message when said security module has accepted or refused a cryptogram of an application.

14. Method according to the claim 1 wherein the cryptogram is transmitted to the security module at the same time as the application is loaded into the equipment via the execution environment of the applications.

15. Method according to claim 1 wherein the application, once loaded into the equipment from the control server via the network, requests a cryptogram from the server at the time of its initialization and transmits said cryptogram to the security module, the confirmation message of acceptance or refusal of the cryptogram being transmitted by the security module to the server via the application.

16. Method according to claim 1, wherein the equipment is a Pay-TV decoder or a computer to which the security module is connected.

17. Security module comprising resources intended to be accessed locally by at least one application installed in an equipment connected to a network, said equipment comprising means for reading and transmission data comprising at least the identifier of the equipment and the identifier of the security module, said module further comprises means for reception, storage and analysis of a cryptogram containing among other data, a digest of said application and instructions), as well as means for verification of said application, and means for extraction and execution of the instructions contained in the cryptogram releasing or blocking certain resources according to the result of the verification of the application.

18. Security module according to claim 17 being of the "subscriber module " or " SIM card" type intended to be connected to a mobile equipment.